MAT 347Y: Groups, rings, and fields
Homework #11.
Due on Friday, January 30 at 10:10am in class

1. In $\mathbb{Z}[i]$, let $\alpha = 47 - 13i$ and $\beta = 53 + 56i$. Find a generator δ of the ideal (α, β). Also, find $\lambda, \mu \in \mathbb{Z}[i]$ such that $\delta = \lambda\alpha + \mu\beta$.

   Hint: Use the Euclidean algorithm in $\mathbb{Z}[i]$. This is described on Example 3 on pages 271-272 of the book.

2. Let $A \subseteq \mathbb{R}$. Let R be an integral domain. We define an *A–polynomial with coefficients in R* as a formal expression of the form

$$r_1 X^{a_1} + \ldots + r_n X^{a_n},$$

   where $n = 0, 1, 2, \ldots$; $a_i \in A$ for all i; $a_i < a_j$ if $i < j$; $r_i \in R$ for all i; and X is a formal variable. By definition, the above expression is 0 when $n = 0$. We denote $R_A[X]$ the set of all such formal expressions.

   For example, $R_{\mathbb{N}}[X]$ is the usual set of polynomials with coefficients in R. As another example,

$$6X^{-1} - 5X^{2/3} + 3X^7$$

   is a $\mathbb{Q}$–polynomial with coefficients in $\mathbb{Z}$.

   Assume now also that A is closed under addition and that $0 \in A$. We can define addition and multiplication of A-polynomials just as we do for regular polynomials. In particular, $R_A[X]$ is an integral domain.

   For every positive integer N, let Y_N be the set of non-negative rational numbers whose denominator is a divisor of 2^N. Let Y be the set of non-negative numbers whose denominator is a power of 2 (including $2^0 = 1$). Finally, define

$$B = \mathbb{C}_Y[X], \qquad B_N = \mathbb{C}_{Y_N}[X].$$

   Our goal is to study the arithmetic of B. Notice first that $B_N \subseteq B_{N+1}$ and that

$$B = \bigcup_{N=1}^{\infty} B_N.$$

   (a) Prove that $B_N \cong \mathbb{C}[X]$ for all N.

   (b) Find all the units of B.

   (c) Let k be a positive integer. Prove that X can be written as the product of k elements in B, none of which is a unit.

(d) Prove that B is not a UFD.

(e) Prove that B is a Bézout domain.

(f) Find a non-principal ideal of B.

(g) Prove that B does not have any irreducible element. (*Hint:* Use the fundamental theorem of algebra, i.e., that every irreducible polynomial with coefficients in $\mathbb{C}$ has degree 1.)

3. In this exercise, we want to solve the diophantine equation $x^2 + xy + y^2 = n$. In other words, we want to answer: For which positive integers n there exist $x, y \in \mathbb{Z}$ such that $x^2 + xy + y^2 = n$? The process is similar to solving the diophantine equation $x^2 + y^2 = n$ (read "Factorization in the Gaussian integers" on pages 289-292 of the book, or see the worksheet with the same name from Friday, January 23 in class.)

   Let us call $\omega = \dfrac{1 + \sqrt{-3}}{2}$.

   (a) Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

   (b) Given a general element $\alpha := x + y\omega \in \mathbb{Z}[\omega]$ with $x, y \in \mathbb{Z}$, calculate its norm $N(\alpha)$.

   Notes: For the definition of the norm in this domain, if you need it, see page 229-230 of the book. We know that $\mathbb{Z}[\omega]$ is a Euclidean domain with this norm (see problem 8a on section 8.1 of the book; you do not need to write this proof now).

   (c) Find all the units in $\mathbb{Z}[\omega]$.

   (d) We proved that for a prime p in $\mathbb{Z}$, the following three statements are equivalent:

      i. p is also a prime in $\mathbb{Z}[i]$,

      ii. the equation $x^2 + y^2 = p$ has no solutions

      iii. $p \equiv 3 \pmod 4$.

   Come up with a similar statement (and prove it) when we replace condition 3(d)ii with "the equation $x^2 + xy + y^2 = p$ has no solutions".

   Suggestion: There is a similar condition to 3(d)iii, but it is not mod 4. To guess what it is, first try to solve the diophantine equation by mere case checking for the first few primes. Once you have guessed what the condition is, go on and try to prove it.

   The following facts may come in handy: $X^3 - 1 = (X - 1)(X^2 + X + 1)$, and this can be even further factored if we allow coefficients in $\mathbb{Z}[\omega]$.

   (e) For which positive integers n does the equation $x^2 + xy + y^2 = n$ have integer solutions?

   (f) Find all solutions to the equation $x^2 + xy + y^2 = 273$.